SOFTWARE ASSURANCE HIGHLIGHTS

March 2012

Software Security Automation and Measurement News

With Department of Homeland Security (DHS) Software Assurance (SwA) Program sponsorship and MITRE technical lead:

- 380 new Common Vulnerabilities and Exposures (CVE) Identifiers were added to the public CVE List in February for a total of 49,649 usable identifiers now available. A total of 127 products to-date from 70 organizations are now recognized as Officially CVE-Compatible.
- A total of eight organizations are now hosting repositories of Open Vulnerability and Assessment Language (OVAL) content in addition to the main OVAL Repository hosted by MITRE. A total of 17 products to-date from 12 organizations are now recognized as Official OVAL Adopters. A total of 23 organizations to-date have made Declarations to Adopt OVAL for 32 products and services.
- A total of 13 products to-date from five organizations are now recognized as Officially CWE-Compatible. A total of 29 organizations to-date have made Declarations of CWE Compatibility for 47 products and services.
- The "**OVAL Language Sandbox**" is on GitHub.com to provide a collaborative environment for OVAL Community Members to propose and fully investigate and implement new capabilities for the language before they are included in an official release. This will ensure that only mature and implementable constructs are added to the OVAL Language. The OVAL Language Sandbox includes the following: Issue Tracking for entering and tracking bugs, bug fixes, and new feature requests; File Distribution for all OVAL Language Sandbox downloads; a Git Repository for anonymous, read-only access; a Wiki, which will be the primary source for information about the OVAL Language Sandbox; and a link to the OVAL Developer Email Discussion List for all OVAL Language Sandbox-related help requests. The OVAL Language Sandbox is free for the public to join at https://github.com/OVALProject/Sandbox. The OVAL Web site was updated on April 5 with an "OVAL Language Sandbox Introductory" page describing the benefits of the sandbox to the community. It describes the sandbox development and mitigation processes and provides a link to the "OVAL Language Sandbox" on GitHub.com.
- We posted a working draft of the OVAL Language UNIX Component Data Model Specification document for community review and comment on the OVAL Version 5.10.1 page with the April 5 OVAL Web site. The specification is the platform-specific extension of the OVAL Language Data Model for UNIX operating systems.
- Common Attack Pattern Enumeration and Classification (CAPEC) Version 1.7 was posted for the public on March 26 on the CAPEC Web site. Changes for the new release include: 14 new patterns; 30 existing patterns fleshed out to Complete status; modification of the Attack_Motivation_Consequences structure to a more expressive one that aligns with the Common_ Consequences structure of the Common Weakness Enumeration (CWE) List, which included conversion of existing content in 187 patterns; mappings to CWE updated for 39 patterns; and minor typographical and content fixes across a limited number of patterns. There are now 474 total attack patterns listed. A detailed report is available for the public that lists specific changes between Version 1.6 and Version 1.7.
-

International Standards for Programming Language Vulnerabilities

MITRE attended the quarterly meeting of International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Joint Technical Committee (JTC) 1/SC 22/WG 23. The central document, ISO/IEC TR 24772, 2nd Edition, Programming Language Vulnerabilities, is currently undergoing its first formal technical ballot. Therefore, by rule, discussion was not permitted at the meeting. It is anticipated that the second edition will be published during 2013. The meeting was devoted to the discussion of new work and prospective new work. A thorough review was performed on the working draft for a recently initiated new project, ISO/IEC 17960, Code Signing for Source Code. In addition, there was a briefing of possible new work on Core Enterprise Security Application Programming Interfaces.

IEEE Adopts ISO/IEC Software Life Cycle Processes

The Institute of Electrical and Electronics Engineers (IEEE) approved the adoption of three ISO/IEC documents, further harmonizing the collection of IEEE with the international standards for software and systems engineering. One, ISO/IEC 24774, is a guide that explains how processes should be described. Two others, ISO/IEC 24748-2 and ISO/EC 24748-3, are guides to the use of ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207, the key life cycle process standards for systems and software, respectively.

SOFTWARE ASSURANCE HIGHLIGHTS

March 2012

Software Assurance Summer Working Group Sessions at MITRE, McLean VA the week of June 26th

The SwA Summer Working Group Sessions will be held June 26 - 28, 2012 at MITRE in McLean, Virginia. The event is open to the public and FREE, but registration is required. You may use this link to register and for more details: https://buildsecurityin.us-cert.gov/bsi/events/1363-BSI.html. There is no cost to attend, but registration is required. Send name, phone, organization, country of citizenship, and email address to: softwareassurance@asballiance.com. Event and logistical information are also on the "Build Security In" website.

GAO Report on IT Supply Chain: National Security-Related Agencies Need to Better Address Risks.

GAO recommended that the federal agencies take steps, as needed, to develop and document policies, procedures, and monitoring capabilities that address IT supply chain risk. Reliance on a global supply chain introduces multiple risks to federal information systems. These risks include threats posed by actors—such as foreign intelligence services or counterfeiters—who may exploit vulnerabilities in the supply chain and thus compromise the confidentiality, integrity, or availability of an end system and the information it contains. This in turn can adversely affect an agency's ability to effectively carry out its mission. Released March 2012, the report is available at http://www.gao.gov/assets/590/589568.pdf.

The SwA Community already has resources to enable the management of risks to the IT/Software Supply Chain. These include recommendation for changes to documents that address these risks in the Systems Engineering Life Cycle (SELC). SwA Community members have co-authored the Software Engineering Institute's (SEI) software security supply chain report http://www.sei.cmu.edu/library/abstracts/reports/10tn016.cfm which is cited in the GAO report http://www.gao.gov/assets/590/589568.pdf.

Software IDs are among the best counter-measures for mitigating risks of counterfeit software. ISO/IEC 19770-2:2009, Information technology -- Software asset management -- Part 2: Software identification tag (under SC7 Software and Systems Engineering) establishes specifications for tagging software to optimize its identification and management. See http://www.iso.org/iso/catalogue_detail.htm?csnumber=53670

To address the issues with unqualified software service providers, the SwA program provides models and standards for guiding process improvement and benchmarking organizational capabilities to deliver secure products, including practices for mitigating risks attributable to malicious insiders. See https://buildsecurityin.us-cert.gov/swa/proself_assm.html

SwA supports also counter-measures for determining if software has malware, vulnerabilities, or exploitable weaknesses with SwA-sponsored security automation associated with MAEC, CVE, and CWE. This includes due-diligence and contracting terms and conditions that address how suppliers determine and assert assurance claims relative to their software being free of malware (MAEC), publicly reported vulnerabilities (CVE), and exploitable weaknesses (CWE) that put the user in the respective mission/business most at risk. See https://buildsecurityin.us-cert.gov/swa/acqart.html#rfp and https://buildsecurityin.us-cert.gov/swa/measurable.html

"Securing a Mobile World" -- the theme of the March/April 2012 issue of CrossTalk

Co-sponsored by DHS NCSD, the Mar/Apr CrossTalk has articles, many about SwA-sponsored efforts:

- iPhone Malware Paradigm by A.K. Sood and RJ. Enbody
- A Practical Approach to Securing and Managing Smart Devices by S. Rai, P. Chukwuma and R. Cozart
- Mobile Applications Security: Safeguarding Data in a Mobile Device World by S.C. Mitchem, S.G. Dykes, Ph.D., S.W. Cook, and J.G. Whipple
- Engaging the Community: Strategies for Software Assurance Curricula Outreach by C.A. Sledge, Ph.D
- The PC Evolution and Diaspora by J.A. Sena, Ph.D.
- New ISO/IEC Technical Report Describes Vulnerabilities in Programming Languages by J.W. Moore, J.Benito, and L. Wagoner
- Supply Chain Risk Management: Understanding Vulnerabilities in Code You Buy, Build, or Integrate by P.R. Croll.

For these articles, go to http://www.crosstalkonline.org/

ICSQ to Hold a Two Day SwA Track

The International Conference on Software Quality 2012 will host two full days of SwA presentations. The conference this year is October 30-31, 2012 in Indianapolis, Indiana with pre-conference tutorials on October 29, 2012. The website is www.icsq.com.

SOFTWARE ASSURANCE HIGHLIGHTS

March 2012

SwA Fall 2012 Forum Call for Participation

Proposals are welcome for the Fall 2012 Software Assurance Forum during the week of September 17, 2012 at MITRE-1, 7525 Colshire Drive, McLean, Virginia 22102. DHS CS&C NCSD is co-sponsoring this event with the Department of Defense (DoD) Office of the Secretary of Defense (OSD) and National Institute for Standards and Technology (NIST) Information Technology Laboratory. The SwA Forum brings together members of government, industry, and academia with vested interests in software assurance to discuss and promote integrity, security, and reliability in software. Progress updates on relevant programs and initiatives will be presented. If you are implementing practical solutions to problems related to examining alternatives to mitigate security risks attributable to software, then you should attend the Software Assurance Forum to better understand what others are doing and extend your network of collaborators.

We are soliciting submissions in a number of different categories for this SwA Forum. We are especially interested in submissions that address the applied technology and lessons learned in the area of Software Assurance. DHS is not providing financial support for SwA participants. Please send an email to software.assurance@dhs.gov if you are interested in participating.

IEEE SWEBOK V3 review

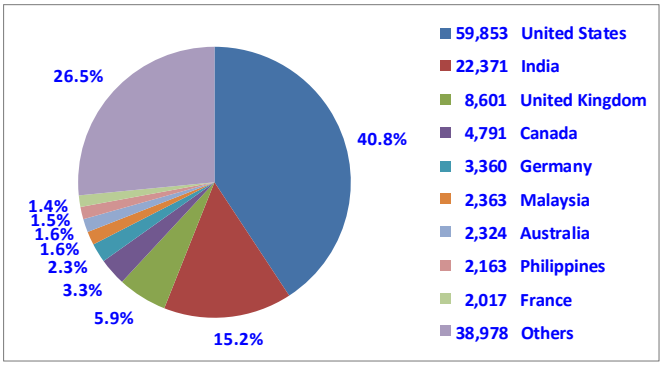
The IEEE Computer Society is now soliciting public review comments on three knowledge areas (KAs) for Version 3 of the Guide to the Software Engineering Body of Knowledge (SWEBOK V3). SWEBOK V3 is an update to the 2004 version of the SWEBOK Guide, which is also known as Technical Report ISO/IEC TR 19759. The 15 KAs in SWEBOK V3 are being published incrementally as they become available for review. Three new KAs are now available for review (Software Engineering Methods and Models, Software Maintenance, and Mathematical Foundations). These KAs can be reviewed and comments can be submitted at: http://computer.centraldesktop.com/swebokv3review/. The SwA Community can still influence the SWEBOK to get SwA properly reflected. Please send an email to software.assurance@dhs.gov with your comments so that we can follow up.

Call for Comments on SwA Pocket Guides

The SwA Pocket Guides at https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html are free, downloadable documents on SwA in acquisition and outsourcing, SwA in development, the SwA life cycle, and SwA measurement and information needs. SwA Pocket Guides are developed collaboratively by participants in the SwA Forum and Working Groups, which function as a stakeholder community that welcomes additional participation in advancing and refining software security. The SwA team has requested a call for comments and suggestions on the following pocket guides: "*Architecture and Design Considerations for Secure Software*," "*Secure Coding*," and "*Requirements Analysis for Secure Software.*" The current drafts of the pocket guides have significant updates compared to the ones on the Community Resource and Information Clearinghouse. Contact Software.Assurance@dhs.gov to receive current drafts of these recently revised pocket guides.

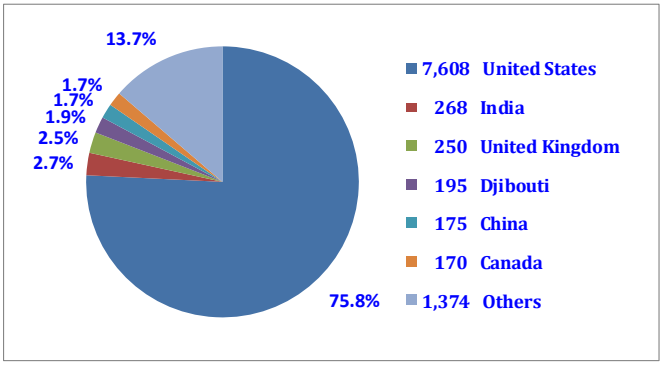
SwA Web site Statistics

Build Security In (BSI) Pageviews by Country



The majority of visitors to the BSI web site are from US locations with India and the United Kingdom in second and third place.

SwA Community Resources and Information Clearinghouse (CRIC) Pageviews by Countries

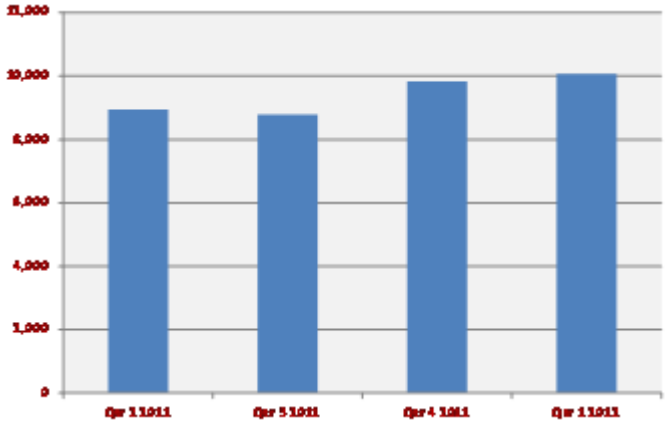


Three quarters of the visitors to the CRIC web site are from US locations with India and the United Kingdom ranking distant second and third place.

SOFTWARE ASSURANCE HIGHLIGHTS

March 2012

CRIC Pageviews by Quarters



CRIC pageviews have shown over 10 percent growth during the past year; the total CRIC pageviews are seven percent of those for the BSI web site.

2012 Software Identification Summit

DHS Software Assurance Program Deputy Director Richard Struse is giving the keynote presentation at the 2012 Software Identification (SWID) Summit. He will explain the role of SWID in the promulgation of the Trusted Automated eXchange of Indicator Information (TAXII) framework and the ITU-T recommended Cybersecurity Information Exchange Framework (X.1500) that references and advocates the use of CVE, CPE, CCE, CAPEC, CWE, MAEC, CEE, OVAL, ARF, and CWSS efforts, as well as CVSS, XCCDF, and IODEF.

This year's summit focuses on software security and software publisher benefits of TagVault.org certified software identification (SWID) tags. Industry experts will give detailed presentations on the issues and risks related to software assurance, and how certified ISO SWID tags can be used to improve the ability for consumers to mitigate these issues and risks. We will also go into detail about how software publishers benefit by including TagVault.org certified SWID tags with their software products.

There is a training day on May 3, 2012 primarily focused on providing information to software publishers on how certified SWID tags can be easily, quickly, and painlessly added to your software products in order to meet the growing customer demand for better and more accurate identification data.
Date: May 2, 2012
Location: Campbell, California
Website: http://tagvault.org/2012-summit

24th Annual Systems & Software Technology Conference (SSTC 2012)

The SwA Community spoke at SSTC 2012:

- Software Assurance v. Security Compliance: Why is Compliance Not Enough? – Dr. Carol Woody (SEI)
- Multi-Perspective Application Security Risk Analysis: A Toolbox Approach – Sean Barnum (MITRE)
- Risk Analysis and Measurement with CWRAF – Bob Martin (MITRE) and Joe Jarzombek (DHS)
- Standards and Guidance for Engineering Secure Systems – Paul Croll (CSC)

In its 24th year, the Systems and Software Technology Conference explored various technologies that will allow us to enhance, advance, and modernize the software-intensive systems that have become pervasive in our defense portfolio. Website: http://sstc-online.org

Secure SDLC 2012 – International Information Systems Security Certification Consortium (ISC)²

Bob Martin, Principal Engineer, MITRE, will speak on The Software Industry's "Clean Water Act" Alternative. Joe Jarzombek will address Software Assurance: Enhancing Cyber Security through Software Supply Chain Risk Management. The (ISC)2 Secure SDLC 2012 Conference will arm software professionals with the latest tools and information regarding application security. Attendees would be individuals that are involved in software development who design, code, build, deploy and manage software. This event will be free for (ISC)2 members, and will be $99 for non-members.
Date: May 17, 2012
Location: DoubleTree by Hilton Washington DC – Crystal City
Website:
https://www.isc2.org/eventdetails.aspx?id=8065

OWASP Monthly Security Blitz

The Open Web Application Security Project (OWASP) is starting a monthly security blitz to rally the security community around a particular topic. The topic may be a vulnerability, defensive design approach, technology or even a methodology. All members of the security community are encouraged to write blog posts, articles,

patches to tools, and videos in the spirit of the current monthly topic. OWASP's goal is to show a variety of perspectives on the topic from the different perspectives of builders, breakers and defenders. April's blitz is on SQL injection. http://owasp.blogspot.com/2012/04/owasp-security-blitz-april-injection.html

OWASP Cheat Sheet Series

1. Do you have a friend with a session management problem? Trouble with input validation or output encoding? The OWASP Prevention Cheat Sheet Series https://www.**owasp**.org/index.php/**Cheat_Sheets** was created to provide a concise collection of high value information on specific web application security topics. These cheat sheets were created by multiple application security experts and provide excellent security guidance in an easy to read format. However, if you are in need of advice about where to look for help, send Security101@lists.owasp.org your questions about application security.

Software Assurance Education, Training & Certification Web Guide

Last month we reported the new Pocket Guide for Software Assurance Education, Training & Certification was out in hard copy. This month we are pleased to report that lead author Dr. Robin Gandhi has posted a web-based version of this Pocket Guide at http://faculty.ist.unomaha.edu/rgandhi/swa/. This version will supplement version on the CRIC at https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html#lifecycle

SwA Websites Offer More Content

The DHS-sponsored websites "Build Security In" https://buildsecurityin.us-cert.gov/bsi and Software Assurance Community Resources & Information Clearinghouse https://buildsecurityin.us-cert.gov/swa were updated with collaboratively developed material.

Do you have questions about Software Assurance? Check out our LinkedIn group Software Assurance Mega-Community at http://www.linkedin.com/groups?gid=1776555

Provide updates on activities important to the SwA Community by emailing software.assurance@DHS.GOV

SOFTWARE ASSURANCE HIGHLIGHTS

March 2012

Quarterly Metrics for Software Assurance Automation

Measure		FY12Q2 Jan-Mar 2012	Total (all years)
# of ID's created for:			
	CVE	1,067	49,639
	OVAL	1525	14,423
	CWE	0	886
	CAPEC	14	549
Subtotals		**2,606**	**65,497**
# of repository updates to:			
	CVE	1,864	113,037
	OVAL	477	7,996
	CWE	0	6,120
	CAPEC	77	128
Subtotals		**2,418**	**127,281**
# of schema updates for:			
	CWE	0	10
	OVAL	1	19
	CAPEC	1	8
	MAEC	1	4
	CybOX	1	3
Subtotals		**4**	**44**
# of tools/services/repositories adopting:			
	CVE	13	298
	OVAL	3	48
	CWE	4	60
Subtotals		**20**	**406**

# of website visitors for:		(Jan12-Mar12)	last year (Apr11-Mar12)
	CVE	554,730	1,825,276
	OVAL	144,945	434,888
	CWE	102,233	510,924
	CAPEC	26,559	116,255
	MAEC	12,168	47,674
Subtotals		**840,635**	**2,935,017**
# of new subscribers for lists:			
	CVE	0	152
	OVAL	27	971
	CWE	39	594
	CAPEC	19	257
	MAEC	16	302
	CybOX	32	32
Subtotals		**133**	**2,308**
# of NIST SP's & inter-agency reports referencing:			
	CVE	2	6
	OVAL	4	9
	CWE	1	3
	CAPEC	0	1
	MAEC	0	1
Subtotals		**7**	**20**
# of Stds, consortia guides & best practice referencing:			
	CVE	5	9
	OVAL	5	14
	CWE	1	25
	CAPEC	0	13
	MAEC	0	1
Subtotals		**11**	**62**

The DHS NCSD Software Assurance (SwA) Program leads efforts in software security automation, diagnostics, measurement, and indicator information sharing efforts through its sponsored projects for Common Attack Pattern Enumeration and Classification (CAPEC), Malware Attribute Enumeration and Characterization (MAEC), Cyber Observables (CybOX), Common Vulnerabilities and Exposures (CVE), Open Vulnerability and Assessment Language (OVAL), and Common Weakness Enumeration (CWE) that includes the Common Weakness Risk Analysis Framework (CWRAF) and Common Weakness Scoring System (CWSS). The Program provides the infrastructure for public-private community collaboration and advances relevant standards, education and training, and it provides resources to reduce software vulnerabilities; share information, and improve capabilities to routinely develop, acquire and deploy resilient software products and services. See "Making Security Measurable" http://measurablesecurity.mitre.org, "Build Security In" https://buildsecurityin.us-cert.gov/bsi, and SwA Community Resources & Information Clearinghouse https://buildsecurityin.us-cert.gov/swa,